AF
IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of
Peyravian et al.

Serial No.: **09/458,922**

Filed: **December 10, 1999**

For: **Time Stamping Method Employing User Specified Time**

Attorney's Docket No: **4541-003**

Patent Pending

Examiner: Beemnet W. Dada

Group Art Unit: 2135

Confirmation No.: 9481

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☒ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief Patents, Commission for Patents, P.O. Box 1450, Alexandria, VA 22313-1450..

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) 273-8300.

May 26, 2006 — Kathleen Koppen
Date — Kathleen Koppen

APPEAL BRIEF

This Appeal Brief is being timely filed within one month of the mailing date of the Notice of Panel Decision from the Pre-Appeal Brief Review. As such, no extension of time fees should be due. The Commissioner is authorized to charge the requisite fee pursuant to 37 C.F.R. §41.20 and any additional fees required or due for entry of this Brief to IBM's Deposit Account No. 09/0461.

(1) REAL PARTY IN INTEREST

The real party in interest is IBM Corp., the assignee of the present invention.

(2) RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences to the best of Applicants' knowledge.

(3) STATUS OF CLAIMS

A total of thirty (30) claims numbered 1-30 have been presented for examination, all of which are pending. The Examiner has allowed claims 1-12 and 19-30. However, the Examiner has finally rejected claims 13-18. Accordingly, Applicant appeals the final rejection of claims 13-18.

(4) STATUS OF AMENDMENTS

All amendments have been entered to the best of Applicants' knowledge.

(5) SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates to a time-stamping protocol for time-stamping digital documents so that the time-stamped document can later be verified. The claimed invention presumes the existence of a trusted outside agency (TSA). *E.g., Spec.*, pg. 4, ll. 1-5.

A document originator creates a time stamp receipt by combining a document or identifying data associated with the document (e.g., a unique hash value), and a time indication. Optionally, the time stamp receipt may also include data such as an identification number associated with the document originator and a sequence number. *E.g., Spec.*, pg. 6, ln. 10 – pg. 7, ln. 2. After creating the time stamp receipt, the document originator forwards the time stamp receipt to TSA for validation. *E.g., Spec.*, pg. 7, ll. 3-5. Upon receipt, the TSA computes an age value for the time stamp receipt by determining a difference between the time indication included in the time stamp receipt and a current time obtained from a trusted clock. *E.g., Spec.*, pg. 7, ll. 15-20. If the computed age value falls within a specified range of the current date and time, the TSA cryptographically binds the time stamp receipt using, for example, a private key. *E.g., Spec.*, pg. 7, ln. 20 – pg. 8, ln. 13. A copy of the bound time stamp receipt is then sent to the document originator, and may later be used by the public to verify the document. *E.g., Spec.*, pg. 8, ll. 13-17.

(6) GROUNDS OF REJECTION

The Examiner finally rejected claims 13-18 under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,393,566 to Levine (hereinafter "Levine").

(7) ARGUMENTS RELATING TO THE §102(e) GROUND OF REJECTION

A. Levine fails to anticipate claim 13.

Claim 13, the sole rejected independent claim, is directed to a computer-implemented method for time stamping a digital document. Claim 13 recites, "creating a time stamp receipt including identifying data associated with said document *and a time indication* ... [and] ... transmitting *said time stamp receipt* to an outside agency." In other words, the time stamp receipt transmitted to the outside agency already includes both the identifying data (e.g., a hash of a document) *and a time indication*. For reference, claim 13 appears below in its entirety.

> 13. A computer-implemented method for time stamping a document comprising:
> creating a time stamp receipt including identifying data associated with said document and a time indication;
> transmitting said time stamp receipt to an outside agency; and
> cryptographically binding at said outside agency said identifying data and said time indication.

There are at least two reasons why the §102 Levine-based rejection of claim 13 fails. First, Levine does not disclose transmitting a time stamp receipt that includes both identifying data and a time indication to an outside agency. In contrast, Levine discloses an authenticating agency that adds a time stamp to the document *after* the agency receives the document. Second, in making the rejection, the Examiner modifies the network structure of the authenticating agency such that it is rendered unusable for its intended purpose. Thus, Levine does not support the Examiner's stated basis for the rejection.

Regarding the first point in more detail, the authenticating agency in Levine includes two computers – a "front" or "public" machine and a "back" or "private" machine. The authenticating agency receives time-stamp requests via the public machine, which is connected to the Internet. The requests include data associated with a document to be time-stamped and signed by the authenticating agency. The private machine then downloads the data associated with the request from the public machine over a secure link, applies a digital signature to the data, and returns the signed message to the public machine for transmission to the requesting party. *Levine*, col. 3, ln. 31 – col. 4, ln. 8.

The authenticating agency in Levine adds a time stamp to the data *after* the agency receives the data from the requesting party. This fact is undeniable.

> The time of the "front" computer is continuously available to any user on the Internet in a number of standard formats including NTP. Any user may request the time in any standard format as often as desired and can compare that time with UTC time information to verify the accuracy of the time-stamping performed by the front machine.

Levine, col. 3, ll. 47-53 (emphasis added).

> FIG. 2 shows the server process carried out on the public machine 10 upon reception of input mail. This process is started by the operating system of the public machine whenever a message is received for time-stamping. ...When the end of the message text is received a time-stamp is added at step 22 and stored with the text.

Levine, col. 6, ll. 9-19 (emphasis added); *see also*, col. 5, ll. 39-65. These passages make clear that whatever data is transmitted to the authenticating agency does not include a time indication. The time indication is added by the authenticating agency, and therefore necessarily cannot occur until *after* the document is transmitted to the authenticating agency.

Even the Examiner supports this fact. "[The] Examiner would point out that Levine teaches creating the hash code of the message *and the time stamp* in the private machine." *Advisory Action*, p. 2, ll. 3-4 (emphasis added). The private machine referred to by the Examiner is, as stated above, part of the authenticating agency. Thus, if the private machine creates the time stamp as the Examiner admits, the authenticating agency of Levine must have already received the document at the public machine and the private machine without a time stamp.

Second, the Examiner stated basis for the rejection is that the authenticating agency does not require the public machine. Rather, the public machine could be any computing device connected to the Internet that time stamps a document prior to sending it to the private machine of the agency.[1] However, Levine does not support such an assertion. Levine specifically employs the public machine at the authenticating agency to isolate the private machine (which is also part of the authenticating agency) from malicious attacks and other access by the general public. *Levine*, col. 7, ln. 57 – col. 8, ln. 9. Levine even discloses a private protocol between the public and private machines to ensure this isolation. *Levine*, col. 5, ll. 47-56; Figure 1.

> Another advantage of the system is that a message which is submitted to the public machine by E-mail will have time-stamps and routing information added to it so that the message that is actually signed will differ from that which was submitted by the sender. The time-stamp and the routing information added to the message as it travels the Internet system are unpredictable from the point of view of the submitter. In that fashion, the message to be signed cannot be completely specified by the submitter which may help to foil certain types of attacks against the procedure.

Levine, col. 8, ll. 10-19 (emphasis added).

Levine simply does not support the Examiner's assertion that the disclosed authenticating agency does not require the public machine. It does. Levine clearly discloses that time stamps transmitted to the authenticating agency are unpredictable and cannot be trusted. Thus, Levine necessarily requires the public machine to be located *at the authenticating agency* for the method to operate as disclosed. Removing the public machine from the realm of the authenticating agency as proposed by the Examiner would alter the operation of the authentication to a point such that it would render it unusable for its intended purpose.

Levine plainly and explicitly situates both the public machine and the private machine within the realm of the authenticating agency. Whatever information is transmitted between these machines is therefore transmitted within the authenticating agency, and thus, cannot be transmitted to the authenticating agency. Whatever information is received at the front machine

[1] The Examiner stated this contention during the telephonic interview conducted December 20, 2005. See

is transmitted to the authenticating agency, and that information, as explicitly disclosed by Levine does not include a time indication "that cannot be trusted."

Anticipation under §102 requires the disclosure of each and every limitation of a claimed invention in a single piece of prior art. *Rockwell Intern. Corp. v. U.S.,* 147 F.3d 1358, 47 U.S.P.Q.2d 1027 (Fed. Cir. 1998). In the instant case, Levine does not disclose, "transmitting said time stamp receipt [that includes a time indication] to an outside agency" as recited by claim 13. Accordingly, the §102 rejection of claim 13 and each of its dependent claims 14-18 fail as a matter of law.

Conclusion

For the reasons set forth above, Levine fails to anticipate claims 13-18 under §102. Accordingly, all claims 13-18 being appealed herein are patentable over the cited art. The Board is respectfully requested to overturn the §102 rejection.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

Dated: May 26, 2006

Stephen A. Herrera
Registration No.: 47,642
Telephone: (919) 854-1844

Applicants' Response to Final Office Action dated December 21, 2005, pg. 2 ¶2.

(8) CLAIMS APPENDIX

1. A computer-implemented method for time stamping a document comprising:

receiving a time stamp receipt at an outside agency, said time stamp receipt including identifying data associated with said document and a time indication;

validating said time stamp receipt at said outside agency by comparing the time indication in said time stamp receipt to the current time; and

if said time stamp receipt is valid, binding at said outside agency said identifying data and said time indication using a cryptographic binding scheme.

2. The time stamping method of claim 1 further including transmitting said binding information to a designated party.

3. The time stamping method of claim 1 wherein said identifying data comprises a digital representation of at least a portion of said document.

4. The time stamping method of claim 3 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

5. The time stamping method of claim 4 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.

6. The time stamping method of claim 1 wherein said time stamp receipt further includes an identification number associated with the document originator

7. The time stamping method of claim 6 wherein said time stamp receipt further includes a sequential record number.

8. The time stamping method of claim 7 wherein the step of validating said time stamp receipt includes comparing said identification number and sequential record number with data maintained by the outside agency.

9. The time stamping method of claim 1 wherein said binding step includes signing a combination of said identifying data and said time indication using a digital cryptographic signature scheme.

10. The time stamping method of claim 1 wherein said binding step includes computing a message authentication code on a combination of said identifying data and said time indication using a secret key controlled by said outside agency.

11. The time stamping method of claim 1 wherein said binding step includes computing a hash value on a combination of said identifying data and said time indication.

12. The time stamping method of claim 1 wherein said binding step includes encrypting a combination of said identifying data and said time indication using a secret key controlled by said outside agency.

13. A computer-implemented method for time stamping a document comprising:

creating a time stamp receipt including identifying data associated with said document and a time indication;

transmitting said time stamp receipt to an outside agency; and

cryptographically binding at said outside agency said identifying data and said time indication.

14. The time stamping method of claim 13 wherein said identifying data comprises a digital representation of at least a portion of said document.

15. The time stamping method of claim 13 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

16. The time stamping method of claim 15 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.

17. The time stamping method of claim 13 wherein said time stamp receipt further includes an identification number associated with the document originator.

18. The time stamping method of claim 14 wherein said time stamp receipt further includes a sequential record number.

19. A computer-implemented method for time stamping a document comprising:

creating a time stamp receipt including identifying data associated with said document and a time indication;

transmitting said time stamp receipt to an outside agency;

validating said time stamp receipt at said outside agency by comparing the time indication in said time stamp receipt to the current time; and

if said time stamp receipt is valid, binding at said outside agency said identifying data and said time indication using a cryptographic binding scheme to generate a certified time stamp receipt.

20. The time stamping method of claim 19 further including transmitting said binding information to a designated party.

21. The time stamping method of claim 19 wherein said identifying data comprises a digital representation of at least a portion of said document.

22. The time stamping method of claim 21 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

23. The time stamping method of claim 22 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.

24. The time stamping method of claim 19 wherein said time stamp receipt further includes an identification number associated with the document originator

25. The time stamping method of claim 24 wherein said time stamp receipt further includes a sequential record number.

26. The time stamping method of claim 25 wherein the step of validating said time stamp receipt includes comparing said identification number and sequential record number with data maintained by the outside agency.

27. The time stamping method of claim 19 wherein said binding step includes signing a combination of said identifying data and said time indication using a digital cryptographic signature scheme.

28. The time stamping method of claim 19 wherein said binding step includes computing a message authentication code on a combination of said identifying data and said time indication using a secret key controlled by said outside agency.

29. The time stamping method of claim 19 wherein said binding step includes computing a hash value on a combination of said identifying data and said time indication.

30. The time stamping method of claim 19 wherein said binding step includes encrypting a combination of said identifying data and said time indication using a secret key controlled by said outside agency.

(9) EVIDENCE APPENDIX

There is no further evidence not contained in the prosecution history.

(10) RELATED PROCEEDINGS APPENDIX

There are no related proceedings.